GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

17/IT

WP 252

# Parere 03/2017 sul documento intitolato "Trattamento dei dati personali nel contesto del sistema di trasporto intelligente cooperativo (C-ITS)"

**adottato il 4 ottobre 2017**

**Indice**

Questo gruppo è stato istituito ai sensi dell'articolo 29 della direttiva 95/46/CE. Esso è un organo consultivo europeo indipendente sulla protezione dei dati e sul rispetto della vita privata. I suoi compiti sono descritti nell'articolo 30 della direttiva 95/46/CE e nell'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e cittadinanza dell'Unione) della Commissione europea, direzione generale Giustizia, B -1049 Bruxelles, Belgio, ufficio MO-59 03/075.

Sito Internet: http://ec.europa.eu/justice/data-protection/index_en.htm

**Indice**

**1 Introduzione ... 3**
**2 Il concetto di C-ITS ... 3**
**3 Sintesi del documento di lavoro sul C-ITS ... 4**
3.1 Dati personali ... 4
3.2 Basi giuridiche ... 5
**4. Parere del Gruppo di lavoro Articolo 29 ... 6**
4.1 Quadro giuridico ... 6
4.2 Dati personali / identificazione degli interessati ... 6
4.3 Rischi per la privacy ... 8
4.4 Liceità del trattamento ... 9
4.5 Sicurezza ... 12
**5 Azioni richieste ... 14**

# 1 Introduzione

Il documento intitolato "Trattamento dei dati personali nel contesto del C-ITS" redatto dal gruppo di lavoro sulla protezione dei dati e sulla privacy della piattaforma del Sistema di trasporto intelligente cooperativo (C-ITS) è stato presentato formalmente al Gruppo di lavoro Articolo 29 il 10 luglio 2017.

La piattaforma del C-ITS è un'iniziativa della direzione generale della Mobilità e dei trasporti della Commissione europea, che è stata varata alla fine del 2014 con la creazione di gruppi di lavoro specializzati, ciascuno dei quali impegnato nello studio di vari aspetti della diffusione del C-ITS, dalla sicurezza alla normalizzazione tecnica fino alla protezione dei dati.

Lo scopo del documento è quello di fornire informazioni di base sul trattamento dei dati personali nel contesto del C-ITS e di chiedere un parere al Gruppo di lavoro Articolo 29 al fine di migliorare il livello di protezione dei dati all'interno di queste nuove tipologie di applicazione.

Il Gruppo di lavoro Articolo 29 è stato invitato dalla Commissione a partecipare con i suoi delegati a una serie di riunioni preparatorie, prima di emanare il presente parere.

Il Gruppo di lavoro Articolo 29 apprezza l'opportunità di essere coinvolto nella discussione con i relativi portatori d’interessi sin dalla fase iniziale di sviluppo di questo nuovo concetto tecnologico e segnalerà quindi alcuni elementi di preoccupazione riguardanti il regolamento generale sulla protezione dei dati (GDPR), che costituirà il quadro giuridico in vigore al momento dell'introduzione della soluzione C-ITS.

Il Gruppo di lavoro Articolo 29 accoglie con favore la recente risoluzione sulla protezione dei dati in veicoli automatici e connessi del convegno ICD PPC svoltosi a Hong Kong dal 25 al 29 settembre 2017, ribadendo le disposizioni ivi contenute.

# 2 Il concetto di C-ITS

Il C-ITS è una soluzione *inter pares* per lo scambio di dati tra veicoli e altre infrastrutture di trasporto (segnaletica stradale o altre stazioni di trasmissione/ricezione) senza l'intervento di un operatore di rete.

Il concetto del sistema è che i pari possono fornirsi a vicenda direttamente informazioni circa il proprio stato (elaborando i dati raccolti dai sensori di cui sono dotati), ricevendo in cambio informazioni analoghe e consentendo così la creazione di un quadro generale (per ogni conducente) dello stato dell'ambiente circostante il veicolo o l'impianto infrastrutturale. Sulla base di tali comunicazioni, l'aspettativa è che si potranno fare migliori previsioni circa le situazioni di traffico e sarà possibile migliorare la prevenzione degli incidenti.

Il C-ITS si basa sulla radiodiffusione costante. Il sistema crea comunicazioni *ad hoc* e non richiede di stabilire una comunicazione permanente o di vincoli tra i pari.

Sono due le tipologie di messaggi che vengono scambiati nell'ambito del C-ITS: i c.d. messaggi CAM (*Cooperative Awareness Messages*) trasmessi con continuità e contenenti dati cinematici oltre alle dimensioni del veicolo, e i messaggi DENM (*Decentralised Environmental Notification Messages*) cioè messaggi decentrati di notifica ambientale inviati

in aggiunta ai messaggi CAM solo al verificarsi di eventi specifici (come ad esempio incidenti) per situazioni di emergenza urgenti e contengono informazioni sull'evento.
I messaggi CAM e DENM prevedono la firma crittografata, che garantisce alla parte ricevente che i messaggi sono stati inviati da un mittente affidabile. La distribuzione di certificati tra i pari avviene utilizzando un'architettura di Infrastruttura a chiave pubblica (PKI). L'infrastruttura PKI è una struttura di governance in cui ogni certificato è associato, in un determinato momento, in modo univoco a un veicolo e dimostra che il veicolo in questione è riconosciuto dal sistema e può essere considerato affidabile.

Nella sua strategia relativa al C-ITS, la Commissione europea ha già individuato diversi casi di utilizzo per la diffusione iniziale (applicazioni del giorno uno). Tali casi, come specificato nel documento sul C-ITS redatto dal gruppo di lavoro sulla protezione dei dati e sulla privacy, sono principalmente connessi alle funzioni informative (quali gli avvisi di lavori stradali in corso, le condizioni meteo ecc.). In questi casi, il conducente ha sempre il totale controllo del veicolo ed è responsabile delle azioni dello stesso. Nel lungo periodo, e con un maggiore livello di automazione, si prevede che l'impatto del C-ITS aumenterà, in quanto il sistema potrebbe gradualmente prendere decisioni di guida al posto del conducente.

Il Gruppo di lavoro Articolo 29 si concentrerà esclusivamente su queste capacità iniziali delle applicazioni del C-ITS. Quando saranno implementati livelli di automazione più elevati, sorgeranno nuovi interrogativi, altamente pertinenti, circa l'impatto sulla libertà e sui diritti dei cittadini dell'UE. Il Gruppo di lavoro Articolo 29, e nel tempo il Comitato europeo per la protezione dei dati, valuteranno tali questioni in una fase successiva. Il Gruppo di lavoro Articolo 29 coglie l'occasione per incoraggiare un dialogo tempestivo tra i pertinenti portatori d’interessi sulle implicazioni per la protezione dei dati di questi scenari futuri, anche considerando le difficili questioni etiche sollevate da un nuovo, incisivo intervento su azioni tradizionalmente gestite dall'uomo.

# 3 Sintesi del documento di lavoro sul C-ITS

## *3.1 Dati personali*

Il gruppo di lavoro sulla protezione dei dati e sulla privacy del Sistema di trasporto intelligente cooperativo riconosce che i messaggi trasmessi, scambiati dai veicoli, costituiscono dati personali. Questa conclusione scaturisce fondamentalmente da due osservazioni: 1) i messaggi contengono certificati di autorizzazione, rilasciati dalla PKI, associati univocamente al mittente; 2) i messaggi contengono titolo, data, dati localizzazione e le dimensioni del veicolo.

Il documento qualifica il meccanismo in atto per lo scambio di messaggi CAM e DENM con i rispettivi certificati digitali come un trattamento di dati pseudonimizzati, sostenendo che le informazioni aggiuntive (l'associazione fra il titolare del certificato e i dati del veicolo) vengono conservate separatamente dai dati dell'utilizzatore (queste informazioni sono tenute dalle autorità di certificazione). Pertanto, a norma dell'articolo 4, paragrafo 5, del GDPR, per identificare gli interessati sarebbero necessarie informazioni aggiuntive. Ecco perché il documento sostiene che si dovrebbe applicare l'articolo 11 del GDPR (trattamento che non richiede l'identificazione). Il documento, tuttavia, non affronta il trattamento effettuato da autorità di certificazione e non fornisce dettagli tecnici sull'infrastruttura PKI, fondamentali per garantire che i dati scambiati siano praticamente pseudonimi.

## *3.2 Basi giuridiche*

Il gruppo di lavoro sulla protezione dei dati e sulla privacy della piattaforma C-ITS conclude che la liceità del trattamento potrebbe non essere fondata solo su una base giuridica, bensì su una combinazione di due o più basi giuridiche, tenendo conto della tempistica e al fine di introdurre la nuova tecnologia nel 2019. In sintesi, il gruppo di lavoro sul C-ITS ritiene che le possibili basi giuridiche adeguate, o una combinazione delle stesse, tenendo presente la natura delle applicazioni del giorno uno, potrebbero essere:

- interesse pubblico (articolo 6, paragrafo 1, lettera e), GDPR);
- esecuzione di un contratto (articolo 6, paragrafo 1, lettera b), GDPR);
- consenso (articolo 6, paragrafo 1, lettera a), GDPR);
- legittimo interesse (articolo 6, paragrafo 1, lettera f), GDPR).

Il gruppo di lavoro sul C-ITS rileva che al fine di applicare l'interesse pubblico come base giuridica, la necessità di questo tipo di trattamento deve essere stabilita in una legge nazionale o dell'UE. Tale base potrebbe essere prevista nell'attuazione della strategia dell'UE per la sicurezza stradale, l'efficienza dei trasporti e la sostenibilità ambientale. La direttiva 2010/40/UE sui sistemi di trasporto intelligenti consente alla Commissione europea di adottare specifiche vincolanti in questo campo attraverso atti delegati. Il gruppo di lavoro sul C-ITS ritiene che l'utilizzo obbligatorio del C-ITS sia un'opzione, ma non applicabile alla diffusione iniziale del sistema nel 2019.

Il gruppo di lavoro del C-ITS ha valutato l'opzione del trattamento dei dati personali ove ciò sia necessario per eseguire un contratto di cui l'interessato è parte. Secondo le conclusioni raggiunte dal gruppo di lavoro del C-ITS, l'applicabilità di questa base giuridica potrebbe non essere generica. Il ricorso a questa base giuridica è possibile in scenari specifici, ad esempio quando l'interessato ha effettivamente un contratto con un operatore stradale privato per poter percorrere tale strada. Il gruppo di lavoro del C-ITS rileva che esiste una catena di soggetti coinvolti nel quadro del C-ITS (case automobilistiche, sviluppatori di software, gestori delle strade). Essi possono essere contitolari del trattamento secondo la definizione dell'articolo 26 del GDPR. Per poter prendere a fondamento la base giuridica della necessità di eseguire un contratto, è necessaria una valutazione dei ruoli delle varie entità in relazione alle finalità e ai mezzi.

Per quanto riguarda la base giuridica del consenso, il gruppo di lavoro del C-ITS studia i vincoli tecnici rappresentati dal tipo di trasmissione delle comunicazioni. Nel contesto del C-ITS, i soggetti che svolgono il ruolo di titolari del trattamento dei dati potrebbero non avere un rapporto diretto con l'interessato. L'interessato non conosce e non può conoscere l'identità di tutti i destinatari dei propri messaggi, visto il modo in cui lo standard è concepito[1]. Il gruppo di lavoro del C-ITS, tuttavia, suggerisce la possibilità di contrassegnare i messaggi CAM e DENM trasmessi in modo da poter codificare le preferenze degli utenti.

Il gruppo di lavoro del C-ITS ha inoltre valutato il trattamento ai fini dei legittimi interessi del titolare del trattamento. Per poter prendere a fondamento questa base giuridica, il titolare del trattamento deve garantire che il trattamento non prevalga sugli interessi o sui diritti

[1] ETSI EN 302 637-2 *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service* e ETSI EN 302 637-3 *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralised Environmental Notification Basic Service*

fondamentali e sulle libertà dell'interessato. Sono molti i vincoli, espressamente riconosciuti nel documento, che ostacolano l'applicabilità di questa base giuridica. Innanzitutto, la necessità di identificare di chi è l'interesse che viene perseguito nella catena di responsabilità del C-ITS, lo svolgimento di verifiche potenzialmente separate da parte di ciascuno dei soggetti coinvolti – in base ai rispettivi ruoli – e secondariamente, l'attuazione di specifiche garanzie aggiuntive per limitare l'impatto sugli interessati.

# 4. Parere del Gruppo di lavoro Articolo 29

## *4.1 Quadro giuridico*

L'applicazione iniziale del sistema di trasporto intelligente cooperativo è prevista per il 2019. Il quadro giuridico pertinente per il trattamento dei dati personali in relazione al C-ITS è quindi il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [...]" (GDPR), entrato in vigore il 25 maggio 2016, che sarà applicabile a partire dal 25 maggio 2018.

Inoltre, in futuro potrà diventare pertinente il nuovo regolamento sulla vita privata e le comunicazioni elettroniche. Secondo la proposta della Commissione europea (COM(2017)10)[2], le comunicazioni da macchina a macchina dovrebbero rientrare nell'ambito di applicazione di questo regolamento.

## *4.2 Dati personali / identificazione degli interessati*

Il gruppo di lavoro del C-ITS ha rilevato correttamente che i dati trasmessi tramite il C-ITS sono dati personali in quanto si riferiscono agli interessati identificati o identificabili. Gli interessati possono essere identificati in vari modi. Innanzitutto, mediante i certificati ottenuti dall'infrastruttura PKI, in quanto tali certificati saranno unici fin dalla progettazione, al fine di distinguere inequivocabilmente il veicolo in cui sono installati. Secondariamente, mediante i dati relativi all'ubicazione, poiché è nota la loro capacità di identificazione[3]: bastano pochi punti in un percorso per distinguere con estrema precisione un individuo in una popolazione, tenendo conto dei modelli di mobilità generalmente regolari delle persone.

Ciò vale soprattutto per i messaggi CAM. I messaggi DENM includono anche ticket di autorizzazione e dati che descrivono un evento specifico. A seconda di come si verifica l'evento (ad es. la densità della zona, il particolare giorno o la dinamica della catena di eventi), tali messaggi possono anche rendere identificabile l'interessato.

Sull’applicabilità dell’articolo 11 del GDPR, il Gruppo di lavoro Articolo 29 desidera esprimere le seguenti preoccupazioni. Nell'articolo 11 si legge che vi sono operazioni di trattamento per le quali l'identificazione dell'interessato non è necessaria – o non è più necessaria – e il titolare del trattamento non è obbligato a identificare l'interessato al solo fine di rispettare il GDPR. Questo articolo va interpretato come un modo per far valere il "vero" principio della riduzione al minimo dei dati, senza tuttavia ostacolare l'esercizio dei diritti

[2] Proposta legislativa della Commissione europea COM(2017)10 relativa al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche [...] (regolamento sulla vita privata e le comunicazioni elettroniche), gennaio 2017. Cfr. anche il Parere WP247 del Gruppo di lavoro Articolo 29, URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

[3] Gruppo di lavoro Articolo 29, WP X, parere 05/2014 sulle tecniche di anonimizzazione.

degli interessati. L'esercizio di tali diritti deve essere reso possibile con l'aiuto di "ulteriori informazioni" fornite dall'interessato. Invocando l'articolo 11 del GDPR senza specificare quali ulteriori dati sono necessari per consentire l'identificazione degli interessati, si impedisce *di fatto* l'esercizio dei diritti di questi ultimi (accesso, rettifica, portabilità, ecc.). Ad ogni modo, i dati pseudonimizzati sono dati personali per definizione (cfr. l'articolo 4 del GDPR), in quanto sono dati relativi a un soggetto identificabile (cfr., in particolare, il considerando 26 del GDPR).

Il Gruppo di lavoro Articolo 29 invita quindi il gruppo di lavoro del C-ITS a presentare proposte sul concetto di "informazioni aggiuntive" che possono essere fornite nel contesto di questo nuovo servizio per rendere tale disposizione efficace, tenendo conto ad esempio degli specifici dati del veicolo o della natura altamente identificabile dei dati di ubicazione. Il gruppo di lavoro rifiuta qualsiasi interpretazione dell'articolo 11 che miri a ridurre la responsabilità del titolare o dei titolari del trattamento per rispettare gli obblighi di protezione dei dati.

I dati personali trattati attraverso il C-ITS possono anche includere particolari categorie di dati, secondo quanto definito nell'articolo 10 del GDPR, connessi a una violazione della segnaletica (ad esempio la "violazione della segnaletica / della sicurezza a un incrocio" nel testo). Queste categorie particolari di dati possono essere trattate nel C-ITS e trasmesse ad altri veicoli. L'articolo 10 del GDPR specifica che i dati relativi alle condanne penali e ai reati possono essere trattati soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Le applicazioni del giorno uno, quindi, dovrebbero essere modificate per evitare la raccolta e la trasmissione di qualsiasi informazione che potrebbe rientrare nell'articolo 10.

Il gruppo di lavoro individua diverse possibilità tecniche per ridurre al minimo i rischi di reidentificazione.

Innanzitutto, è possibile migliorare la politica di emissione dei certificati PKI. Fintantoché un certificato è valido, è possibile identificare e localizzare un veicolo, e la localizzazione a corto raggio è una componente di progettazione importante del C-ITS. La localizzazione a corto raggio consente una stretta connessione causale fra la viabilità stradale e i veicoli che si spostano nella zona in questione, ed è quindi considerata necessaria per attivare il sistema e far funzionare le applicazioni. Al fine di evitare la localizzazione prolungata, che non è essenziale ai fini della sicurezza stradale, i titoli di autorizzazione vengono modificati col tempo. Mentre il gruppo di lavoro del C-ITS sottolinea la necessità di non modificare troppo spesso i titoli di autorizzazione, al fine di limitare il consumo di certificati e di non vanificare la facile identificazione dei pericoli e delle avvertenze circa i conducenti nelle vicinanze, il Gruppo di lavoro Articolo 29 raccomanda invece di valutare attentamente le possibilità di una frequenza più elevata per limitare i rischi di una localizzazione prolungata.

Secondariamente, occorre regolare la frequenza di trasmissione dei messaggi CAM.
Secondo le impostazioni di frequenza dei messaggi di CAM proposte, sarebbe possibile localizzare i veicoli nel raggio di pochi metri. Ciò è possibile ad esempio se diversi segmenti di sequenze molto fitte di punti con indicazione temporale – che possono essere localizzati ad esempio su una mappa – sono "colorati" in modo diverso mediante un certificato specifico (supponendo che ciascun certificato sia visivamente di un colore diverso). L'affermazione formulata nel documento dal gruppo di lavoro del C-ITS, secondo la quale "colorare in modo diverso" (cioè attribuendo certificati diversi a) questi segmenti sulla mappa impedirebbe a un

osservatore di ricostruire l'intero percorso di un veicolo, è discutibile. I dati sulla mobilità sono intrinsecamente e fortemente correlati, oltre che molto ripetitivi per la maggior parte dei conducenti, perciò riunire segmenti apparentemente disgiunti per ricomporre un percorso integro non dovrebbe essere considerato eccessivamente difficile per un aggressore dotato di mezzi e motivazione. Inoltre, quando un veicolo cambia il proprio certificato è comunque possibile collegare il nuovo certificato a quello vecchio: qualsiasi altro veicolo nelle vicinanze del veicolo che cambia certificato potrà testimoniare la scomparsa del vecchio certificato e la comparsa di quello nuovo, e potrà quindi collegarli fra loro. Il gruppo di lavoro del C-ITS dovrebbe affrontare questo problema per evitare tali correlazioni.

In terzo luogo, il Gruppo di lavoro Articolo 29 sottolinea l'importanza del principio di riduzione al minimo dei dati per mitigare i rischi di reidentificazione, anche attraverso l'applicazione di rimedi quali la generalizzazione o l'introduzione di "rumore"[4]. Tali rimedi possono essere progettati in modo da non compromettere il quadro complessivo delle condizioni ambientali e la possibilità di individuare un nuovo pericolo limitando, al contempo, un'inutile esposizione o una localizzazione prolungata del conducente. Occorre prestare particolare attenzione alla generalizzazione o all'introduzione di rumore per quanto riguarda le proprietà statiche dei veicoli al fine di ridurre il rischio di localizzazione mediante l'identificazione delle proprietà del veicolo.

## *4.3 Rischi per la privacy*

Il Gruppo di lavoro Articolo 29 riconosce che il concetto alla base del C-ITS può recare benefici ai conducenti, fornendo migliori livelli di usabilità e consapevolezza ambientale, e per il grande pubblico migliorando la sicurezza stradale e tutelando la sicurezza di altri automobilisti e pedoni. Tuttavia, il Gruppo di lavoro Articolo 29 evidenzia che l'utilizzo su larga scala di questa nuova tecnologia, che comporterà la raccolta e il trattamento di quantitativi di dati senza precedenti sull'ubicazione degli individui in Europa, pone nuove sfide ai diritti fondamentali e alla protezione dei dati personali e della privacy sia degli utenti sia di altri individui che potrebbero essere danneggiati.

Innanzitutto, per definizione il C-ITS rivelerà ciò che non eravamo abituati a divulgare: dove guidiamo e il modo in cui guidiamo. Mediante le funzionalità di trasmissione e ricezione dei veicoli, queste informazioni personali verranno trasmesse pubblicamente a qualsiasi veicolo nelle vicinanze. Si tratta di una forma di localizzazione comportamentale permanente distribuita che può generare uno sgradevole senso di sorveglianza furtiva.

La mancanza di trasparenza è un altro importante rischio per la privacy. Attraverso i loro veicoli, gli utenti diventeranno emittenti continui. Essi devono essere pienamente consapevoli della portata del trattamento, degli altri pari con i quali si scambiano dati nell'ambiente C-ITS (altri veicoli, case automobilistiche, gestori delle strade, altri soggetti pubblici o privati) e di come essi trattano questi dati.

La scelta della trasmissione tra pari per distribuire i messaggi, invece delle comunicazioni dirette, rappresenta un'altra sfida: i messaggi possono essere ricevuti da un numero illimitato di entità, le cui intenzioni e la cui capacità tecnologica non sono e non possono essere note al mittente. Ciò causa un'asimmetria informativa fra i mittenti e gli altri pari (destinatari) del C-ITS. Tale asimmetria deve essere riequilibrata con un maggior livello di controllo sui dati personali.

---

[4] Cfr. gli esempi nel Gruppo di lavoro Articolo 29, WP216, parere 05/2014 sulle tecniche di anonimizzazione.

I dati cinematici e i dati sull'ubicazione saranno molto preziosi per diverse parti interessate con varie intenzioni e finalità – da inserzionisti a case automobilistiche e compagnie di assicurazione. L'accesso illimitato e indiscriminato ai dati condivisi all'interno del C-ITS può consentire l'illegittimo accumulo di singoli profili di movimento, una "datificazione" dei comportamenti di guida su cui possono essere modellati, pubblicizzati e venduti prodotti e servizi personalizzati.

I dati sulla mobilità possono risultare altrettanto attraenti per l'applicazione della legge e del codice della strada, che va oltre lo scopo per il quale sono stati generati e trattati i dati del C-ITS. Ciò suscita preoccupazioni sulla necessità e la proporzionalità del loro potenziale utilizzo a questi scopi.

Un altro rischio di rilievo che il C-ITS comporta per la protezione dei dati è l'estensione indebita delle funzionalità (*function-creep*). Se l'asimmetria informativa sull'identità degli altri pari, insita nell'architettura di trasmissione scelta, non viene adeguatamente affrontata con strumenti atti a creare fiducia, potrebbe generare delle distorsioni rispetto alla finalità originaria delle comunicazioni, sviando gli utenti verso luoghi non voluti. Ciò può accadere o a causa di previsioni imprecise sullo stato dell'ambiente (ad es. creando un ingorgo anziché ridurre il volume di traffico) o per un'interpretazione non neutra dei dati ambientali (ad es. inducendo gli utenti a visitare determinate zone per interessi economici di uno dei pari).

## *4.4 Liceità del trattamento*

È opportuno sottolineare che il regolamento (UE) 2016/679 non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico (articolo 2 (2) (c)). Tale esenzione può essere valida solo se strettamente limitata al trattamento che ha luogo all'interno dell'auto, ed esclusivamente se il conducente controlla interamente il trattamento effettuato dal dispositivo. Non può invece essere valida quando il dispositivo installato nelle vetture inoltra i dati di altre auto nelle vicinanze, che sia immediatamente o in conseguenza del trattamento locale. In tali casi il trattamento non è limitato a un'attività strettamente personale.

La liceità del trattamento dei dati personali coinvolti nel funzionamento del C-ITS va ricercata nell'articolo 6, paragrafo 1, del GDPR. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

Tenuto conto dello scopo del C-ITS di migliorare la sicurezza stradale, promuovere l'efficienza dei trasporti e la sostenibilità ambientale, anche attraverso l'implementazione di questo sistema di interoperabilità in tutta Europa, il Gruppo di lavoro Articolo 29 ritiene che la base giuridica a lungo termine per questo tipo di trattamento sia l'adozione di uno

strumento giuridico a livello di UE (articolo 6, paragrafo 1, lettera c), del GDPR). In vista della futura prevalenza di automobili a guida (semi-)automatica, è probabile che verrà il momento in cui l'introduzione di questa tecnologia nei veicoli diventerà obbligatoria al pari dell'obbligo giuridico per le case automobilistiche di includere funzionalità di eCall in tutti i nuovi veicoli. Tale obbligo di legge non dovrebbe permettere la raccolta e il trattamento indiscriminati di dati personali. La portata dell'obbligo giuridico va valutata opportunamente e convalidata se proporzionata e strettamente necessaria in una società democratica, come previsto dalla protezione offerta dai diritti fondamentali applicabili.

La Commissione deve avviare al più presto questo processo di valutazione e l'iter legislativo al fine di evitare che il trattamento dei dati relativi all'ubicazione e di altri dati personali dei cittadini dell'UE all'interno del C-ITS avvenga senza il fondamento di una base giuridica e non sia tutelato interamente da un adeguato livello di protezione.

L'analisi delle altre basi giuridiche tralascia alcuni elementi importanti. In questo esercizio può essere utile una valutazione delle capacità tecniche del C-ITS e del suo ambito di applicazione.

La funzione centrale del C-ITS è costituita dal rilevamento dell'ubicazione, della velocità e della direzione dei veicoli. Quanto maggiore è la frequenza dei messaggi scambiati, tanto più nitida e più dettagliata è la panoramica dei veicoli dell'ambiente circostante e maggiore la capacità di previsione dei pericoli del sistema. Il Gruppo di lavoro Articolo 29 ritiene che il livello di adozione e di conferimento dei dati sia un fattore cruciale per il funzionamento del C-ITS: un contributo di dati insufficiente o una bassa risoluzione della vista ambientale catturata da ogni veicolo potrebbe compromettere o persino rovinare la validità del C-ITS in quanto strumento per la sicurezza stradale.

Tuttavia, incitare i conducenti ad adottare il sistema C-ITS non significa instaurare con la forza un sistema invasivo di localizzazione. La possibilità di beneficiare del C-ITS *di per sé* dovrebbe incentivare i conducenti ad aderire liberamente al C-ITS. In questo modo sarebbe possibile raggiungere in modo naturale una massa critica di utenti affinché il sistema funzioni correttamente senza alcuna imposizione; al tempo stesso, si lascerebbe alle persone la libertà di scegliere se desiderano partecipare al sistema e, in caso affermativo, di selezionare le opzioni di localizzazione (tempi, frequenza, luoghi) che meglio si confanno alle rispettive preferenze.

Il livello di risoluzione della localizzazione è ben rappresentato dagli indicatori di prestazione del sistema[5]:

*Un veicolo genererà un messaggio CAM ogni circa 4 metri e quando il senso di marcia cambia di più di 4°. Quando una distanza tra la posizione corrente e quella passata è cambiata di più di 4 metri o la velocità è cambiata più di 0,5 m/s rispetto all'ultima volta, viene inviato un messaggio CAM, e comunque almeno una volta al secondo e al massimo una volta ogni 0,1 secondi in condizioni normali.*

Queste opzioni di localizzazione costituiscono la base di partenza. Nel documento si legge infatti che *queste sono le specifiche definite attualmente, che possono cambiare a seconda delle effettive necessità delle nuove funzioni emergenti*. Inoltre, secondo il documento, queste

[5] *Processing personal data in the context of C-ITS. Annex I - day one applications, standards & security* (CAM a. 2.2) [Il trattamento dei dati personali nel contesto del sistema di trasporto intelligente cooperativo (C-ITS). Allegato I - Applicazioni del giorno uno, standard & sicurezza].

impostazioni non possono essere modificate dall'utente. Il gruppo di lavoro del C-ITS non trova il giusto equilibrio tra la necessità di promuovere l'adozione del C-ITS e quella di prevenire i comportamenti parassitari – conducenti che non partecipano al sistema ma godono dei suoi benefici –, impostando la frequenza di scambio dei messaggi (e quindi la granularità della localizzazione) al più alto livello possibile.

Il gruppo di lavoro del C-ITS non ha ancora raggiunto un accordo sulla fattibilità tecnica di ottenere il consenso degli interessati. A tale proposito, il gruppo di lavoro sottolinea che devono essere soddisfatte tutte le condizioni per il consenso, come previsto nell'articolo 7 del GDPR e nel considerando 42. I titolari del trattamento devono prestare particolare attenzione alle modalità impiegate per ottenere un consenso specifico, libero e informato da diversi partecipanti quali i proprietari di auto o gli utenti di autovetture. Tale consenso deve essere fornito separatamente, per scopi specifici e non può essere vincolato al contratto di acquisto o noleggio di un'auto nuova; inoltre, il consenso deve essere revocato con la stessa facilità con cui è accordato. Il consenso non costituisce un'adeguata base giuridica nel caso dei dipendenti in quanto il rapporto datore di lavoro-dipendente è caratterizzato da subordinazione giuridica e i dipendenti non sono liberi di negare il consenso.

In particolare, poiché il C-ITS è basato sulla trasmissione continua, non vi sono soluzioni di continuità nella trasmissione per segnalare l'intenzione o i desideri da parte dell'utente. La trasmissione, inoltre, è uno schema di comunicazione proiettato in avanti, senza retroazione, e questo rende impossibile impostare un meccanismo di riconoscimento reciproco tra la persona interessata (mittente) e il titolare del trattamento (destinatario). Tale mancanza di riconoscimento reciproco non dovrebbe, di per sé, escludere l'utilizzo del consenso, ma rende più difficile trattare i dati solo per scopi specifici e ben definiti da parte di titolari del trattamento noti. D'altra parte, l'affermazione contenuta nel documento secondo cui il consenso non può essere considerato come una base giuridica valida perché il titolare del trattamento non è stato definito in questa fase a un livello che consentirebbe all'interessato di conoscerne l'identità, è fuorviante: l'esistenza di titolari del trattamento ben definiti è un presupposto necessario per il trattamento stesso, e nessuna base giuridica a norma dell'articolo 6, paragrafo 1, del GDPR ne giustificherebbe un'identificazione vaga. Lo sforzo tecnico di includere dei contrassegni nella struttura dei messaggi CAM e DENM per segnalare le preferenze degli utenti è un buon punto di partenza, ma non è ancora la soluzione.

Il gruppo di lavoro del C-ITS esamina altresì la possibilità di far valere la necessità di eseguire un contratto (articolo 6, paragrafo 1, lettera b), del GDPR). Un contratto specifico tra un interessato e il titolare del trattamento, separato da qualsiasi altro contratto di acquisto/noleggio di auto, in linea di massima potrebbe consentire al conducente di aderire liberamente al sistema.

Sull'applicabilità dell'opzione del controllo congiunto, previsto dall'articolo 26 del GDPR, vale la pena sottolineare che non si tratta di un gioco di forza tra i contitolari del trattamento, né si intende fornire un margine discrezionale su come prendere accordi al fine di eludere, parzialmente o interamente, gli obblighi sul controllo congiunto. I contitolari del trattamento che hanno un rapporto consolidato con i clienti o con soggetti privati e possono comunicare con loro direttamente, dovrebbero assumersi la piena responsabilità di informarli circa la catena di responsabilità, l'esistenza e gli scopi degli altri contitolari del trattamento.

Se il trattamento è necessario per l'esecuzione di un contratto specifico e liberamente scelto di cui l'interessato è parte, il Gruppo di lavoro Articolo 29 ha ripetutamente chiarito[6] che tale disposizione va intesa in senso stretto e che c'è una chiara connessione tra la valutazione della necessità e della conformità e il principio di limitazione delle finalità. Nel contesto del C-ITS sono due gli aspetti di primaria importanza. Innanzitutto, è importante determinare chiaramente in anticipo le parti coinvolte nel contratto, al fine di limitare il trattamento nel ristretto perimetro dei soli soggetti coinvolti nell'ambito di applicazione del C-ITS ed evitare qualsiasi ulteriore utilizzo dei dati ad opera di altre parti sconosciute. L'esempio riportato nel documento di un contratto tra l'interessato e un operatore stradale privato è incompleto poiché vi possono essere altre parti coinvolte nel trattamento (case automobilistiche e sviluppatori di software, ad esempio) – o in veste di contitolari del trattamento secondo l'articolo 26 del GDPR, o congiuntamente nel contesto di un unico consorzio con il ruolo di titolare del trattamento completo – che possono stipulare un contratto con gli interessati. In secondo luogo, la motivazione, il contenuto e gli obiettivi del contratto devono precedere il trattamento stesso e il titolare o i titolari del trattamento devono verificare rispetto a tale motivazione e a tali obiettivi se il trattamento dei dati è necessario per l'esecuzione del contratto con ogni singolo utente, tenendo conto del fatto che le automobili possono essere guidate dai proprietari o da altri utenti.

In merito all'eventuale applicazione della necessità di trattare i dati per un interesse legittimo (articolo 6, paragrafo1, lettera f), del GDPR), il Gruppo di lavoro Articolo 29 rammenta che questa non dovrebbe essere considerata come "l'ultima spiaggia" per casi complessi nei quali è difficile applicare altre basi giuridiche che giustifichino la liceità del trattamento. L'esito di una verifica potrebbe determinare se l'articolo 6, paragrafo 1, lettera f), del GDPR può essere preso a fondamento per il trattamento. L'identificazione dei titolari del trattamento e dei loro interessi costituisce una condizione preliminare necessaria, come affermato nel documento. Ma vi sono altri fattori di rilievo da considerare[7], in particolare la fonte della legittimità dell'interesse – sia essa radicata nell'interesse pubblico o nell'interesse di uno specifico soggetto –, l'impatto sugli interessati e sulle rispettive aspettative inerenti alla privacy, data anche la natura potenzialmente sensibile dei dati di localizzazione, le tutele aggiuntive – anche da un punto di vista tecnico – che potrebbero limitare qualsiasi indebito impatto su di essi.

## *4.5 Sicurezza*

Il C-ITS si basa sulla radiodiffusione di messaggi. In questo contesto, garantire riservatezza, integrità e disponibilità delle comunicazioni, ovvero la sicurezza delle comunicazioni, richiede maggiori sforzi e ulteriori specifiche rispetto alle comunicazioni dirette.

La radiodiffusione è un modo illimitato per comunicare con destinatari indefiniti, raggiungibili da un dispositivo emittente. Qualsiasi metodo valido per limitare il trattamento delle informazioni trasmesse esclusivamente al contesto dell'applicazione del C-ITS, evitando che possano essere indebitamente trattate da altri destinatari non appartenenti al sistema, si dovrà basare sull'esistenza di pari affidabili e sulla considerazione che l'utilizzo di dati provenienti dal C-ITS per scopi diversi dalla sicurezza stradale costituisce un reato penale.

---

[6] Parere 02/2013 sulle applicazioni per dispositivi intelligenti e parere 06/2014 sull'interesse legittimo del titolare del trattamento a norma dell'articolo 7 della direttiva 95/46/CE.

[7] Parere 02/2014 sul concetto di interessi legittimi del titolare del trattamento a norma dell'articolo 7 della direttiva 95/46/CE.

Vale la pena ricordare che la proposta legislativa COM(2017)10, il regolamento sulla vita privata e le comunicazioni elettroniche, prevede limitazioni estremamente rigide sull'utilizzo di "dati emessi" come i messaggi CAM e DENM, in base alle quali l'articolo 8, paragrafo 2, ne proibisce in generale l'utilizzo, tranne se necessario al solo scopo di stabilire una connessione, per il tempo necessario a stabilirla e allo scopo di stabilirla, e se sono in essere opportune misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato ai rischi, come definito nell'articolo 32 del GDPR.

Il documento evidenzia particolarmente il meccanismo di PKI come un modo per creare fiducia nel sistema C-ITS. In realtà, l'infrastruttura PKI è un modo per distribuire una risorsa specifica di informazioni (nel caso del C-ITS i certificati digitali) nell'ambito di una struttura di governance controllata. La PKI non fornisce alcun meccanismo di esecuzione per stabilire le reali intenzioni dei titolari dei certificati o degli emittenti. Purtroppo, recentemente i casi di collusione o gli incidenti di sicurezza che riguardano le autorità di certificazione sono diventati più frequenti, e ci sono forti incentivi per ottenere certificazioni solo allo scopo di commettere atti dolosi[8].

L'esistenza di un'architettura PKI non garantisce *di per sé* la creazione di fiducia fra pari. Per rafforzare la fiducia occorrono misure aggiuntive. Un elemento importante è l'implementazione di meccanismi volti a garantire la sicurezza. Altri fattori importanti consistono in un controllo scrupoloso e periodico sulle operazioni delle autorità di certificazione, sia sotto forma di controllo incrociato fra autorità di certificazione, sia mediante audit o ispezioni effettuate dalle istituzioni pubbliche che partecipano alla promozione del C-ITS.

Garantire l'integrità significa evitare che i dati possano essere modificati senza autorizzazione, distorcendo il corretto funzionamento di un sistema informativo. Nel contesto della radiodiffusione del C-ITS, ciò può accadere se i pari (persino pari affidabili) manipolano l'immagine dell'ambiente circostante introducendo furtivamente dati falsi o rispondono a un interesse commerciale piuttosto che a un obiettivo pubblico di sicurezza stradale. Filtrare i valori anomali nel flusso dei messaggi CAM e DENM, che potrebbero preannunciare indicatori fuori dalla media, costituisce un valido meccanismo deterrente contro l'uso doloso del C-ITS e un modo per garantire che i dati scambiati siano quelli essenziali allo scopo.

La disponibilità è la capacità delle informazioni di servire al proprio scopo quando è necessario. Si tratta di un attributo molto delicato da garantire in un ambiente di trasmissione per la presenza di un compromesso tra tempo e qualità dei dati. Se l'esistenza (e quindi la disponibilità) di dati correlati a un potenziale pericolo viene generata dalla trasmissione simultanea e massiccia di messaggi su tale situazione, affidarsi a un campione di messaggi troppo ridotto potrebbe generare molti falsi allarmi; d'altra parte, se si aspetta di raccogliere una quantità sufficiente di elementi di prova da numerose fonti diverse potrebbe essere troppo tardi per la sicurezza delle persone. La prevenzione degli incidenti è un risultato molto importante che è atteso dal trattamento di dati personali nel contesto del C-ITS, e il Gruppo di lavoro Articolo 29 raccomanda agli sviluppatori di software di prestare la massima attenzione e di adoperarsi al massimo nella progettazione di programmi software in grado di distinguere i falsi positivi e negativi, anche mediante l'aggiornamento collaborativo dei parametri di servizio, in modo da non generare allarmi o, al contrario, impedire la segnalazione di situazioni veramente pericolose per gli interessati.

---

[8] Edelman, Benjamin. *Adverse Selection in Online 'Trust' Certifications and Search Results.* Electronic Commerce Research and Applications 10, n. 1 (gennaio–febbraio 2011).

# 5 Azioni richieste

Il Gruppo di lavoro Articolo 29 accoglie con favore gli sforzi compiuti dalla Commissione europea e dal gruppo di lavoro sulla protezione dei dati e sulla privacy del Sistema di trasporto intelligente cooperativo per incorporare i principi di protezione dei dati nel funzionamento di queste nuove applicazioni fin dall'inizio.

L'esercizio svolto dal gruppo di lavoro del C-ITS è un buon punto di partenza, ma ha bisogno di essere integrato con una serie di azioni specifiche a diversi livelli. Il Gruppo di lavoro Articolo 29 ritiene particolarmente importanti i seguenti aspetti della protezione dei dati:

- la Commissione dovrebbe attuare regolamenti settoriali per la raccolta e il trattamento dei dati nel campo dei sistemi di trasporto intelligenti;
- la Commissione dovrebbe elaborare una tabella di marcia per il trattamento legittimo dei dati sull'ubicazione dei cittadini dell'UE nel contesto delle applicazioni del C-ITS, con l'obiettivo finale di adottare uno strumento giuridico a livello di UE (articolo 6, paragrafo 1, lettera c), del GDPR);
- l'adozione di tali strumenti giuridici dovrebbe iniziare con una valutazione della necessità e della proporzionalità delle rispettive disposizioni; inoltre, nel corso del processo legislativo si dovrebbe commissionare una valutazione dell'impatto sulla protezione dei dati (articolo35, paragrafo 19, del GDPR) al fine di chiarire i rischi e le misure di mitigazione fin dall'inizio;
- le altre basi giuridiche previste nel documento del gruppo di lavoro del C-ITS (vale a dire consenso, esecuzione di un contratto o legittimo interesse) potrebbero essere prese in considerazione solo se è possibile risolvere le criticità individuate per ciascuna di loro nel presente Parere;
- in una qualsiasi delle basi giuridiche selezionate, l'impostazione predefinita di tutte le funzionalità installate del C-ITS deve essere disattivata;
- si dovrebbero attuare le disposizioni dell'articolo 25 del GDPR (protezione dei dati fin dalla progettazione e protezione per impostazione predefinita) consentendo agli utenti di selezionare le opzioni di localizzazione (tempi, frequenza, luoghi) che meglio si confanno alle rispettive preferenze;
- si dovrebbe rafforzare la sicurezza per limitare il rischio di uso illecito del C-ITS al di là dell'ambito delle finalità legittime;
- si dovrebbero adottare altri rimedi fin dalla progettazione per quanto riguarda la privacy, quali la generalizzazione o l'introduzione di rumore, in modo da non compromettere il quadro complessivo delle condizioni ambientali e la possibilità di individuare un nuovo pericolo limitando, al contempo, un'inutile esposizione o una localizzazione prolungata del conducente;
- si dovrebbe prestare particolare attenzione alla frequenza con cui i certificati vengono modificati, al fine di creare un giusto equilibrio tra la frequenza scelta e i rischi di una localizzazione prolungata;
- non si dovrebbero trasmettere speciali categorie di dati né i dati relativi a reati e condanne penali;

- va valutata attentamente la qualità dei dati al fine di mitigare eventuali rischi di utilizzo non neutro del C-ITS, la generazione di falsi allarmi o, al contrario, l'errata interpretazione di situazioni di reale emergenza;
- il meccanismo della PKI per la distribuzione dei certificati dovrebbe essere documentato pubblicamente in modo dettagliato e strettamente monitorato, al fine di limitare il rischio di collusioni tra autorità di certificazione e pari o l'intrusione di soggetti malevoli;
- si dovrebbero indicare chiaramente i periodi di conservazione dei dati trattati da tutte le parti coinvolte nella piattaforma C-ITS, e dovrebbe essere vietato creare una banca dati centralizzata dei messaggi scambiati dai partecipanti al C-ITS.